UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

ERIC LACERTE, on behalf of himself and all others similarly situated,	)	
Plaintiff,	)	**C.A. No. 11-**
v.	)	
	)	**CLASS ACTION**
GOOGLE, INC.,	)	
	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

I. PRELIMINARY STATEMENT

1. This is a class action for damages for Defendant's violations of: (a) Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511, *et seq.*; and (b) Pennsylvania's Wiretapping and Electronic Surveillance Act, PA ST 18 Pa. C.S.A. § 5703, *et seq*. These laws have long been designed to protect individuals from having their electronic communications intercepted by persons or corporations not authorized to do so.

2. This class action addresses the systemic abuse and misappropriation by Google of private electronic communications by thousands of individuals throughout the United States through the deployment and utilization of its Google Street View internet service. Rather than merely taking panoramic, street view, photographs of every building, lot and home on selected streets throughout the United States, Google's Street View service was actually collecting information sent over open WiFi networks, such as a WiFi device's unique identifier, the Media Access Control ("MAC") address, as well as the Service Set Identifier ("SSID") assigned by

users. In short, rather than taking pictures of public places, Google was surreptitiously collecting private information, which, on information and belief, included e-mails, video, audio, Voice Over Internet Protocol ("VoIP") information and other payload data belonging to users and operators of home-based WiFi networks.

II. JURISDICTION AND VENUE

3. Jurisdiction of this Court arises under 28 U.S.C. § 1331 because this Complaint alleges the violation of a federal statute, 18 U.S.C. § 2511, *et. seq*. Jurisdiction also is conferred upon this Court by the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), in that there is diversity of citizenship between the Plaintiff and members of the proposed Class and Defendant and the aggregate amount in controversy is in excess of five million dollars ($5,000,000.00).

4. Venue lies in this District pursuant to 28 U.S.C. § 1391(b) in that the Defendant transacts business within the District and the conduct complained of occurred in this District.

III. PARTIES

5. Plaintiff Eric Lacerte is an individual residing in Coatesville, Pennsylvania. During all times relevant herein, Lacerte used and maintained an open wireless internet connection at his home which he shares with his wife. Lacerte and his wife used their WiFi connection to access the internet and to conduct both personal and business affairs, including but not limited to, e-mails, research, banking, entertainment, shopping, health matters, and other communications. Mr. Lacerte's home can be seen on Google Maps and Street View. On information and belief, Defendant surreptitiously collected, decoded, and stored data from Mr. Lacerte's WiFi connection, including payload data, on at least one occasion. Mr. Lacerte did not know that Google collected his data, nor did he give permission for Google to do so.

6. Defendant Google, Inc. ("Google") is a Delaware corporation with a principal

place of business in Mountain View, California. Google's self-described mission is to organize the world's information and make it universally accessible. One of Google's services is Google Street View.

IV. FACTUAL ALLEGATIONS

A. Google Street View

7. Google Street View is a technology featured in Google Maps and Google Earth that provides panoramic views from various positions along many streets in the world. It was launched on May 25, 2007, originally only in several cities in the United States, and has since gradually expanded to include more cities and rural areas worldwide.

8. Google Street View displays images taken from a fleet of specially adapted cars. Areas not accessible by car, like pedestrian areas, narrow streets, alleys and ski resorts, are sometimes covered by Google Trikes (tricycles) or a snowmobile. On each of these cars (or other vehicles) there are nine directional cameras for 360° views at a height of about 2.5 meters, GPS units for positioning, three laser range scanners for the measuring of up to 50 meters 180° in the front of the vehicle. Notably, Google also equipped these vehicles with 3G/GSM/WiFi antennas for scanning 3G, GSM and WiFi hotspots.

9. When Google's engineers created the data collection system for its Google Street View vehicles, most commonly known as a packet analyzer or wireless sniffer, they intentionally included computer code in the system that was designed to and did sample, collect, decode, and analyze all types of data sent and received over the WiFi connections of Class members.

10. Having knowingly equipped its Google Street View vehicles with devices capable of intercepting wireless communications over wireless networks it secretly mapped, Google

stored the information it intercepted on its servers where, on information and belief, Google employees, vendors and contractors have access to the intercepted data maintained on Google's servers.

11. The Plaintiff and other wireless internet users, whose information was secretly intercepted by Google, did not and could not give their consent to Google to intercept their data transmissions.

B. Government Investigations and Google's Admissions

12. On April 23, 2010, the German Commissioner for Data Protection and Freedom of Information announced his discovery that Google Street View vehicles were utilizing their antennas and scanners to collect information transmitted from household wireless networks. Google later admitted that its street view vehicles throughout the world, including the United States, were actually capturing payload data, meaning all data consisting of all or part of any documents, e-mails, video, audio and VoIP information being sent over the wireless internet.

13. On April 27, 2010, Google posted an entry on its European Public Policy Blog in response to inquiries from the German Data Protection Authority ("GDPA") concerning the specific data Google Street View vehicles collected. In this post, Google explained that it collected the SSID (the WiFi network name) and MAC address (basically the ID number of the WiFi network's hardware), but did not collect data sent over WiFi networks, *i.e.* payload data. http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html.

14. In May 2010, after the GDPA asked to audit the WiFi data collected by the Google Street View vehicles, Defendant admitted in a blog post that the information in its April 27 post was wrong, and that it indeed had been "collecting samples of payload data from open (*i.e.*, nonpassword-protected) WiFi networks." http://googleblog.blogspot.com/2010/05/wifi-

data-collection-update.html.

15. Defendant further admitted that it had collected and stored "snippets of e-mails and other internet activity" from home wireless networks. http://www.ft.com/cms/s/2/8a23b394-5fab-11df-a670-00144feab49a.html#axzz1GDybGV4Ms. Eric Schmidt, Defendant's chief executive, "admitted that he could not rule out the possibility that personal data such as bank account details were among the data collected." He admitted that "We screwed up. Let's be clear about that."

http://www.ft.com/cms/s/2/db664044-6f43-11df-9f43-00144feabdc0.html#axzz1GDybGV4M.

16. Likewise, Google co-founder Sergey Brin admitted that Google's actions were wrong. Speaking at the Google I/O conference on May 19, 2010, Brin said: "In short, let me just say that we screwed up. I'm not going to make any excuses about it. The answer is yes. We do have a lot of internal controls in place but obviously they didn't prevent this error from occurring."

http://www.zdnet.com/blog/btl/sergey-brin-we-screwed-up-on-wifi datacollection/34759?tag=content;search-results-rivers.

17. After the Google Street View vehicles' wireless sniffers sampled, collected, and decoded these data, Defendant stored the data on its servers. Defendant has admitted that it has collected and stored data from WiFi connections around the world, including the United States. At present, data gathered in the United States has been ordered preserved by a federal court. Pursuant to a motion for a temporary restraining order in *Van Valin, et al. v. Google Inc.*, 3:10-cv-0057-MO (D. Or. filed May 17, 2010), Judge Mosmon issued an Order dated May 24, 2010 requiring Google to "Produce two exact bit-by-bit mirror image copies of the existing hard drive (described by the Defendant as an encrypted hard drive containing the 'payload' data for the

United States), such that upon completion of the process, the target disks are identical to and interchangeable with the existing source disk ('clones')."

18. On June 9, 2010, Google responded to a letter sent by members of the United States House Energy and Commerce Committee, requesting information regarding Street View. In its response, Google confirmed that it "included code in [its] software that collected samples of 'payload data'" and that "[i]t is possible that the payload data may have included personal data if a user at the moment of collection broadcast such information…" Google also stated that it had been "collecting WiFi data via Street View cars in the United States" since 2007. *See* June 9, 2010 Letter to Chairman Waxman, and Representatives Barton and Markey from Pablo Chavez, Defendant's Director of Public Policy.

19. In 2010, former Connecticut Attorney General, Richard Blumenthal, commenced a multistate investigation, on behalf of more than 30 states, into Defendant's "Google Street View cars' unauthorized collection of personal data from wireless computer networks." http://www.ct.gov/ag/cwp/view.asp?Q=461862&A=3869.

20. On January 28, 2011, the Connecticut Attorney General's Office issued a press release regarding its investigation of Google, stating that it was in settlement negotiations with Google regarding Google's collection of personal payload data.

V. CLASS ACTION ALLEGATIONS

21. Plaintiff brings this action individually and as a class action, pursuant to Rules 23(a) and 23(b) of the Federal Rules of Civil Procedure, on behalf of the following Class and Pennsylvania Subclass:

National Class:

> All persons in the United States whose electronic communications sent or received on wireless internet connections were intercepted by Defendant's

> Google Street View vehicles from May 25, 2007 through the present. Excluded from the Class are Defendant, including subsidiaries and affiliates, federal governmental entities and instrumentalities, and the Court and Court personnel.

Pennsylvania Subclass:

> All persons in Pennsylvania whose electronic communications sent or received on wireless internet connections were intercepted by Defendant's Google Street View vehicles from May 25, 2007 through the present. Excluded from this Subclass are Defendant, including subsidiaries and affiliates, federal governmental entities and instrumentalities, and the Court and Court personnel.

22. The Class and Pennsylvania Subclass are so numerous that joinder of all members is impracticable. Upon information and belief, the Defendant has continually intercepted the electronic communications of tens of thousands of persons throughout the United States and the Commonwealth of Pennsylvania. Because the interception practices at issue are a standard and uniform practice employed by Defendant, numerosity may be presumed.

23. There are questions of law and fact common to the Class and Pennsylvania Subclass which predominate over any questions affecting only individual Class members. These questions include:

a) Whether Defendant's interception of wireless electronic communications violated the federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C §§ 2511, *et seq.*;

b) Whether Defendant's interception of wireless electronic communications violated Pennsylvania's Wiretapping and Electronic Surveillance Act, 18 Pa. C.S.A. § 5703, *et seq.*;

c) Whether Defendant acted intentionally in intercepting wireless electronic communications;

d) Whether Defendant should be enjoined from intercepting any electronic

communications from any wireless network without the express consent of the owners of such electronic data;

e) The appropriate statutory damages that should be awarded to the Class and Pennsylvania Subclass; and

f) The appropriate punitive damages that should be awarded to the Class and Pennsylvania Subclass.

24. Plaintiff will fairly and adequately protect the interests of the Class and Subclass. Plaintiff is committed to vigorously litigating this matter and has retained counsel experienced in handling class actions and claims involving unlawful business practices. Neither Plaintiff nor his counsel have any interests which might cause them not to vigorously pursue this claim.

25. This action should be maintained as a class action because the prosecution of separate actions by individual members of the Class and Pennsylvania Subclass would create a risk of inconsistent or varying adjudications with respect to individual members which would establish incompatible standards of conduct for the parties opposing the Class and Pennsylvania Subclass, as well as a risk of adjudications with respect to individual members which would as a practical matter be dispositive of the interests of other members not parties to the adjudications or substantially impair or impede their ability to protect their interests.

26. Google has acted or refused to act on grounds that apply generally to the Class and Pennsylvania Subclass, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class and Pennsylvania Subclass as a whole.

27. A class action is a superior method for the fair and efficient adjudication of this controversy. The interest of Class members in individually controlling the prosecution of separate claims against Defendant is small because the maximum statutory damages available in

an individual action are minimal in comparison to the expense and burden and prosecuting individual litigation. Management of the Class claims is likely to present significantly fewer difficulties than those presented in many class claims.

VI. CLAIMS FOR RELIEF

COUNT I

Wiretap Act, 18 U.S.C §§ 2511, *et seq.* (On Behalf of the National Class)

28. Plaintiff incorporates the foregoing paragraphs as though the same were set forth at length herein.

29. As more fully described herein, beginning at least as early as May 25, 2007, and continuing through the present, Google intentionally sought, intercepted and collected the electronic communications of the Plaintiff and the Class.

30. As a direct and proximate result of such conduct, Google unlawfully intercepted the electronic communications of the Plaintiff and the Class in violation of 18 U.S.C. § 2511.

31. As a result of the above violations, and pursuant to 18 U.S.C. § 2520, Defendant is liable to Plaintiff and the Class in the sum of statutory damages consisting of the greater of $100 a day for each day of violation by the Defendant, or $10,000; injunctive and declaratory relief; punitive damages in an amount to be determined by jury, but sufficient to prevent the same or similar conduct by the Defendant in the future; and, a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT II
Pennsylvania Wiretapping and Electronic Surveillance Act, 18 Pa. C.S.A. § 5703, *et seq.* (On Behalf of the Pennsylvania Subclass)

32. Plaintiff incorporates the foregoing paragraphs as though the same were set forth at length herein.

33. As more fully described herein, beginning at least as early as May 25, 2007, and continuing through the present, Google intentionally sought, intercepted and collected the electronic communications of the Plaintiff and the Pennsylvania Subclass.

34. As a direct and proximate result of such conduct, Google unlawfully intercepted the electronic communications of the Plaintiff and the Pennsylvania Subclass in violation of 18 Pa. C.S.A. § 5703.

35. As a result of the above violations, and pursuant to 18 Pa. C.S.A. § 5725, Defendant is liable to Plaintiff and the Pennsylvania Subclass in the sum of statutory damages consisting of the greater of $100 a day for each day of violation by the Defendant, or $1,000; injunctive and declaratory relief; punitive damages in an amount to be determined by jury, but sufficient to prevent the same or similar conduct by the Defendant in the future; and, a reasonable attorney's fee and other litigation costs reasonably incurred.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays that relief be granted as follows:

A. That an order be entered certifying the proposed Class and Pennsylvania Subclass under Rule 23 of the Federal Rules of Civil Procedure and appointing Plaintiff and his counsel to represent the Class and the Pennsylvania Subclass;

B. That an order be entered declaring that Defendant's actions as described above are in violation of the federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C §§ 2511, *et seq.*;

C. That an order be entered declaring that Defendant's actions as described above are in violation of the Pennsylvania Wiretapping and Electronic Surveillance Act, 18 Pa. C.S.A. § 5703, *et seq.*;

D. That judgment be entered against Defendant for statutory damages, pursuant to 18 U.S.C. § 2520(c)(2)(B);

E. That judgment be entered against Defendant for statutory damages, pursuant to 18 Pa. C.S.A. § 5725;

F. That judgment be entered against Defendant for punitive damages as appropriate, pursuant to 18 U.S.C. § 2520(b)(2);

G. That judgment be entered against Defendant for punitive damages as appropriate, pursuant to 18 Pa. C.S.A. § 5725;

H. That Plaintiff and the Class recover pre-judgment and post-judgment interest as permitted by law;

I. That Plaintiff and the Class be awarded their reasonable attorneys' fees and other litigation costs reasonably incurred, pursuant to 18 U.S.C. § 2520(b)(3);

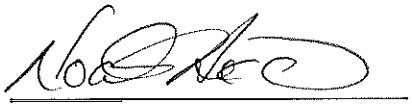
J. That Plaintiff and the Pennsylvania Subclass be awarded their reasonable attorneys' fees and other litigation costs reasonably incurred, pursuant to 18 Pa. C.S.A. § 5725;

K. That the Court enter an Order granting the Plaintiff, the Class, and the Pennsylvania Subclass a preliminary and permanent injunction restraining and enjoining the Defendant from any act to intercept electronic communications and from disclosing to anyone the communications intercepted and stored on its servers; and,

L. That the Court grant such other and further relief as may be just and proper.

Date: March 16, 2011

Respectfully submitted,



Noah Axler, Esq.
Michael D. Donovan, Esq.
DONOVAN SEARLES & AXLER, LLC
1845 Walnut Street, Suite 1100
Philadelphia, PA 19103
(215) 732-6067
mdonovan@donovansearles.com
naxler@donovansearles.com